KAZEROUNI LAW GROUP, APC
Abbas Kazerounian (SBN: 249203)
ak@kazlg.com
David J. McGlothlin (SBN: 253265)
david@kazlg.com
Mona Amini (SBN: 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

BLOOD HURST & O'REARDON, LLP
Timothy G. Blood (SBN: 149343)
Jennifer L. MacPherson (SBN: 202021)
501 West Broadway, Suite 1490
San Diego, California 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101
tblood@bholaw.com
jmacpherson@bholaw.com

Attorneys for Plaintiff,
Teneika Tillis

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

TENEIKA TILLIS, individually an on behalf of all others similarly situated, Plaintiff, vs. FIDELITY NATIONAL FINANCIAL, INC.; AND LOANCARE, LLC, Defendants.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

//

//

//

Plaintiff Teneika Tillis ("Plaintiff"), by and through their undersigned counsel, file this Class Action Complaint on behalf of themselves individually and all others similarly situated, against Fidelity National Financial, Inc. ("FNF") and LoanCare, LLC ("LoanCare") (collectively as "Defendants"). Plaintiff bases the below allegations on personal information and belief, the investigation of counsel, and states the following:

INTRODUCTION

1. Fidelity National Financial (or "FNF"), is a Fortune 500 company that is a leading provider of title insurance and settlement services for the mortgage and real estate industries.[1]

2. On November 21, 2023, FNF disclosed it had been the victim of a "cybersecurity incident." This virtually froze all the company's and its subsidiaries' activities, leaving people buying and selling homes, or paying mortgages, confused and uncertain of what was going to happen to their properties and money.

3. In its Form 8-K report to the Securities and Exchange Commission (SEC), FNF stated it "recently became aware of a cybersecurity incident that impacted certain FNF systems. FNF promptly commenced an investigation, retained leading experts to assist the Company, notified law enforcement authorities, and implemented certain measures to assess and contain the incident." The report further stated FNF's investigation to date "has determined that an unauthorized third party accessed certain FNF systems and acquired certain credentials. The investigation remains ongoing at this time."

4. LoanCare, a nationally recognized leader in full-service subservicing to the mortgage industry,[2] is a Fidelity National Financial Company and direct subsidiary of FNF.[3] LoanCare is the current servicer and/or subservicer of Plaintiff's

[1] https://www.investor.fnf.com/
[2] https://fnf.com/companies/mortgage-real-estate-services/#LoanCare
[3] https://www.loancareservicing.com/about-us/

home mortgage.

5. LoanCare, founded in 1983, provides subservicing services on more than 100,000 loans for ninety companies in all fifty states, making it approximately the seventh largest subservicer in the nation. LoanCare, which generated 2008 revenue of approximately $19 million and adjusted pre-tax earnings of approximately $4.4 million, provides traditional subservicing, outsourced loss mitigation and other servicing related products and services.[4]

6. On November 29, 2023, LoanCare's website (www.myloancare.com) published the following notice for Plaintiff and similarly affected Class members:

> LoanCare's ability to service your mortgage loan has been impacted by a Cybersecurity Incident. Websites at domain myloancare.com are currently offline, however, our call center is available. We are working diligently to resolve the issue as quickly and safely as possible. In the meantime, no late charges will be incurred and there will be no negative credit reporting due to the outage. We will let you know as soon as we're back online. Thanks for your patience and apologies for any inconvenience this may have caused you.

7. Defendants have had prior notice of their inadequate data security procedures and practices. Previously, in August 2022, LoanCare notified its customers of a data breach impacting their sensitive personal information, including debit/credit card number, expiration date, and security code.[5]

8. Defendants have not yet disclosed the total number of customers and clients impacted by the November 2023 "cybersecurity incident" and it is unclear what sensitive personal information and/or PII was disclosed, accessed, and/or acquired from Defendants' systems.

9. Shortly after FNF announced the incident, ransomware group ALPHV (also known as BlackCat) listed FNF on its dark web site, effectively claiming responsibility for the cyberattack, and pressuring FNF into paying a ransom to restore operations.

---

[4] https://www.investor.fnf.com/news-releases/news-release-details/fidelity-national-financial-inc-announces-acquistion-loancare

[5] https://www.mass.gov/doc/assigned-data-breach-number-28110-loancare-llc/download

10. Upon information and belief, Plaintiff's and the Class members' unencrypted personal identifiable information, or PII, which was collected, maintained, and stored by Defendants was acquired, or reasonably believed to have been acquired, by an unauthorized person in the "cybersecurity incident" disclosed by Defendants (the "Data Breach").

11. Because the Data Breach compromised Plaintiff's sensitive personal information, Plaintiff and the Class (defined below) have been placed in an immediate and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach.

12. As a result of Defendants' conduct, Plaintiff and the Class have and will be required to continue to undertake time-consuming and often costly efforts to mitigate the actual and potential harm caused by the Data Breach. This includes efforts to mitigate the breach's exposure of their PII, including by, among other things, placing freezes and setting alerts with credit reporting agencies, contacting financial institutions, closing, or modifying financial accounts, reviewing, and monitoring credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites and applications, and requesting and maintaining accurate records.

13. Plaintiff therefore brings this Class Action seeking relief and damages against Defendants for themselves and all other persons who were similarly impacted by the Data Breach and Defendants' inadequate data security procedures and practices.

JURISDICTION

14. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005. Subject matter jurisdiction is proper because: (1) the amount in controversy in this class action exceeds five million dollars ($5,000,000), excluding interest and costs; (2) there are more than 100 Class members; (3) at least one member of the Class is diverse from

the Defendants; and (4) the Defendants are not a government entity.

15. This Court has personal jurisdiction over Defendants because Defendants' acts or omissions and false or misleading representations regarding the security of Plaintiff's and Class members' PII have impacted Plaintiff, including Plaintiff Tillis, who resides in this district and Defendants do business and transact business in this District.

16. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part events and injury giving rise to Plaintiff's claims occurred in this District and Defendants do business and transact business in this District.

PARTIES

17. Plaintiff Tillis is and has been for all relevant times a resident of Fontana, California. Defendants currently own and/or service Plaintiff Tillis's home mortgage. Upon information and belief, Plaintiff Tillis's PII was compromised by the Data Breach. Since learning of the Data Breach, Plaintiff has spent time and effort monitoring her accounts for identity theft or fraud.

18. Defendant Fidelity National Financial, Inc. is a corporation organized under the laws of Delaware with a corporate headquarters in Jacksonville, Florida while maintaining a mailing address in Irvine, California.

19. Defendant LoanCare, LLC is a limited liability company organized under the laws of Virginia with its principal place of business or headquarters in Virginia Beach, Virginia.

FACTUAL BACKGROUND

A. Defendants Collected, Maintained, and Stored PII.

20. In providing home loan or mortgage servicing and related financial services, Defendants collect sensitive personal information from customers. This information includes name, email address, username, password, social security number, phone number, mailing address, financial information and history,

employment information drivers' license information, insurance information, marital status, and other personal and highly sensitive information a person might provide when trying to procure a home loan or mortgage. Defendants host a large repository of sensitive personal information for its customers and received from its customers, including Plaintiff and the Class.

B. Defendants Knew They Needed to Protect Customers' Sensitive Personal Information and Committed to Protecting their PII.

21. FNF has a Privacy Notice on its website which clearly states that "Fidelity National Financial, Inc. and its majority-owned subsidiary companies (collectively, "FNF," "our," or "we") respect and are committed to protecting your privacy."[6]

22. FNF's Privacy Notice further represents that it "maintain[s] physical, electronic, and procedural safeguards to protect your Personal Information." [7]

23. As a condition of receiving loan servicing and other mortgaging services, FNF collects and requires that its customers turn over highly sensitive personal information. In its "Privacy Notice", FNF makes clear that it will not disclose customers' Personal Information and Browsing Information to nonaffiliated third parties, except as required or permitted by law and under certain circumstances, including to "affiliated or nonaffiliated service providers who provide or perform services or functions on our behalf and who agree to use the information only to provide such services or functions," such as LoanCare. [8]

24. FNF knew it needed to protect the privacy and safeguard the sensitive personal information and PII of Plaintiff and the Class members, and further committed to holding its partners and affiliates, like LoanCare, to the very same privacy protection standards it follows.

[6] https://fnf.com/privacy-notice
[7] *Id.*
[8] *Id.*

25. In an April 27, 2023, proxy statement to shareholders FNF acknowledges that it is "highly dependent on information technology" and further states:

> We are focused on making strategic investments in information security to protect our clients and our information systems. Our investments include both capital expenditures and operating expenses for hardware, software, personnel and consulting services. As our primary solutions and services evolve, we apply a comprehensive approach to the mitigation of identified security risks. We have established policies, including those related to privacy, information security and cybersecurity, and we employ a broad and diversified set of risk monitoring and risk mitigation techniques. [P] Internal audits, external audits, regulatory reviews and self-assessments are conducted to assess the effectiveness and maturity of our Enterprise Risk Management and Information Security Program on a recurring basis. We maintain Miscellaneous Professional Liability insurance which provides coverage for cybersecurity incidents as part of our insurance program.
>
> Our board has a strong focus on cybersecurity. Our approaches to cybersecurity and privacy are overseen by the audit committee. At each regular meeting of the audit committee of our board of directors, our Chief Risk Officer, Chief Compliance Officer, Chief Information Security Officer and Chief Internal Auditor provide reports relating to existing and emerging risks, including, as appropriate, risk assessments, cyber and data security risks and any security incidents. Our audit committee chairman reports on these discussions to our board of directors on a quarterly basis. In addition, our audit committee chairman and one of our other audit committee members have attended third-party director education courses on cybersecurity and privacy issues and trends in recent years.
>
> Our employees are one of our strongest assets in protecting our customers' information and mitigating risk. We maintain comprehensive and tailored training programs that focus on applicable privacy, security, legal and regulatory requirements that provide ongoing enhancement of the security and risk culture at FNF. We continue to provide strong focus on all areas of cybersecurity including threat and vulnerability management, security monitoring, identity and access management, phishing awareness, risk oversight third-party risk management, disaster recovery and continuity management. Our employees participate in annual trainings including: Information Security Training, Records Management: Managing and Safeguarding Records Training and Understanding and Protecting Privacy Training.[9]

[9]https://www.sec.gov/ix?doc=/Archives/edgar/data/0001331875/000110465923051332/tm231872d1_def14a.htm

26. Similarly, in its April 23, 2020, proxy statement to shareholders FNF acknowledged that it is "highly dependent on information technology networks and systems to securely process, transmit and store electronic information" and that "[a]ttacks on information technology systems continue to grow in frequency, complexity and sophistication. Such attacks have become a point of focus for individuals, businesses and governmental entities. These attacks can create system disruptions, shutdowns or unauthorized disclosure of confidential information, including non-public personal information, consumer data and proprietary business information."[10]

C. Defendants' Inadequate Data Security Measures Exposed Customers' Sensitive Personal Information. And PII.

27. In or around November 2023, a malicious actor gained unauthorized access to Defendants' data systems, which included customer databases. By doing so, the actor gained access to the sensitive personal, financial, and other information of FNF and/or LoanCare customers, including Plaintiff and the Class members.

28. Upon information and belief, the actors accessed and acquired substantial amounts of Plaintiff's and the Class's sensitive personal information, including their PII. This data included highly sensitive personal information such as names, addresses, loan information, financial information, and Social Security Numbers.

29. Given that Defendants purposefully obtained and stored the PII of Plaintiff and the Class and knew or should have known of the serious risk and harm caused by a data breach, Defendants were obligated to implement reasonable measures to prevent and detect cyberattacks. This includes measures recommended by the Federal Trade Commission ("FTC") and promoted by data security experts and other agencies. This obligation stems from the foreseeable risk of a data breach

[10] https://www.sec.gov/Archives/edgar/data/1331875/000110465920050323/tm202067-1_def14a.htm

given that Defendants collected, stored, and had access to a swath of highly sensitive consumer records and data and, additionally, because other highly publicized data breaches at different institutions put Defendants on notice that the highly personal data they stored, or allowed other entities to store via a services contract or relationship, might be targeted by cybercriminals.

30. Despite the highly sensitive nature of the personal information Defendants obtained, created, and stored, and the prevalence of data breaches at financial institutions like Defendants or related businesses, Defendants inexplicably failed to implement and maintain reasonable and adequate security procedures and practices to safeguard the PII of Plaintiff and the Class. The Data Breach itself and information Defendants have disclosed about the breach to date, including its length, the need to remediate Defendants' cybersecurity, and the sensitive nature of the impacted data, collectively demonstrate Defendants failed to implement reasonable measures to prevent the Data Breach and the exposure of highly sensitive customer information.

D. Exposure of PII and other Sensitive Personal Information Created a Substantial Risk of Harm.

31. The personal and financial information of Plaintiff and the Class is valuable and has become a highly desirable commodity to data thieves.

32. Upon information and belief, Plaintiff's and the Class members' sensitive personal information and/or PII has been made available on the dark web as a result of the Data Breach.

33. Defendants' failure to reasonably safeguard Plaintiff's and the Class's sensitive PII has created a serious risk to Plaintiff and the Class, including both a short-term and long-term risk of identity theft and other fraud.

34. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without

permission, to commit fraud or other crimes.

35. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[11]

36. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity.

37. Purchasers of PII use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional PII from the victim, as well as PII from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and tangible money, along with unreported emotional harms.

38. The FBI's Internet Crime Complaint (IC3) 2019 report estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help stop fraudulent transactions and mitigate losses.

39. Defendants did not rapidly report to Plaintiff and the Class that their PII had been exposed or stolen, but instead took seven weeks to make a public notice related to the Data Breach, and even that notice did not include the number of impacted victims.

40. The FTC has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour reiterated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be

---

[11] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims,* ThreatPost.com

commercially valuable. Data is currency."[12]

41. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed or can be disposed of pursuant to relevant state and federal laws;

(4) limiting administrative access to business systems;

(5) using industry tested and accepted methods;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function properly;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.[13]

42. The United States Cybersecurity & Infrastructure Security Agency ("CISA"), and other federal agencies, recommend similar and supplemental measures to prevent and detect cyberattacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

43. The FTC cautions businesses that failure to protect PII and the resulting

[12] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable.

[13] *Start With Security, A Guide for Business,* FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money, and patience to resolve the fallout.[14] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures—like Defendants failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

E. Plaintiff's and the Class's PII are Valuable.

44. Birth dates, Social Security Numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.[15]

45. For that reason, cybercriminals on the dark web are able to sell data like Social Security Numbers for large profits.

46. Consumers place a considerable value on their PII and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their PII, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth" between $30.49 and $44.62.[16] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

47. Defendants' Data Breach exposed a variety of Plaintiff's and the Class members' data, including their Social Security Numbers and other sensitive personal information.

---

[14] Taking Charge, What to Do if Your Identity is Stolen, FTC, https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0014-identity-theft.pdf.

[15] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

[16] 11-Horn Hann, Kai-Lung Hui, et al, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf

48. The Social Security Administration ("SSA") warns that a stolen Social Security Number can lead to identity theft and fraud: "Identity thieves can use your number and your credit to apply for more credit in your name."[17] If the identity thief applies for credit and does not pay the bill, it will damage victims' credit and cause a series of other related problems.

49. Social Security Numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

50. Plaintiff and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny. The Class has incurred and will incur this damage in addition to any fraudulent use of their sensitive personal information.

CLASS ALLEGATIONS

51. Plaintiff brings this action on behalf of themself individually and on behalf of all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

> ***All individuals whose data was impacted or otherwise compromised by the Data Breach disclosed or reported by Defendant(s) in November 2023.***

52. Excluded from the class are Defendants and their subsidiaries and affiliates; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

53. Plaintiff reserves the right to, after conducting discovery, modify,

[17] Social Security Administration, Identity Theft and Your Social Security Number, https://www.ssa.gov/pubs/EN-05-10064.pdf

expand, or amend the above Class definition or to seek certification of a class or Classes defined differently than above before any court determines whether certification is appropriate.

54. **Numerosity.** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there are thousands of members of the Class, if not more. The number of impacted individuals remains unknown and unreported, and Plaintiff believe additional entities and persons may have been affected by the Data Breach. The precise number of Class members, however, is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

55. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether Defendants knew or should have known that their data environment and cybersecurity measures, or those created by corporate service providers, created a risk of a data breach;

b. Whether Defendants controlled and took responsibility for protecting Plaintiff's and the Class's data when they solicited that data, collected it, stored it on its servers, and authorized a third party to collect and store that data;

c. Whether Defendants' security measures were reasonable considering the FTC data security recommendations, state laws and guidelines, industry standards, and common recommendations made by data security experts;

d. Whether Defendants owed Plaintiff and the Class a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected, stored, and maintained from Plaintiff and Class members;

e. Whether Defendants' failure to adequately secure Plaintiff's and the Class's data constitutes a breach of its duty to institute reasonable security measures;

f. Whether Defendants' failure to implement reasonable data security measures allowed the breach of their data systems to occur and caused the theft of Plaintiff's and the Class's data;

g. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

h. Whether Plaintiff and the Class were injured and suffered damages or other losses because of Defendants' failure to reasonably protect its data systems; and

i. Whether Plaintiff and the Class are entitled to damages and/or equitable relief.

56. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff are a typical member of the Class. Plaintiff and the Class members are persons who provided data to Defendants, whose data was collected, stored, and maintained by Defendants and resided on Defendants' servers or systems, and whose personally identifying information was exposed in Defendants' Data Breach. Plaintiff's injuries are similar to other Class members and Plaintiff seek relief consistent with the relief due to the Class.

57. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff are an adequate representative of the Class because Plaintiff are members of the Class and are committed to pursuing this matter against Defendants to obtain relief for themselves and for the Class. Plaintiff have no conflicts of interest with the Class.

Plaintiff have also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiff intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

58. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit customers to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

59. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), Defendants, through their conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CAUSES OF ACTION

COUNT I

Negligence

60. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

61. Defendants owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiff and the Class. This duty arises from multiple sources.

62. Defendants owed a common law duty to Plaintiff and the Class to

implement reasonable data security measures because it was foreseeable that hackers would target Defendants' data systems and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and the Class would be harmed. Defendants controlled their technology, infrastructure, and cybersecurity, and to the extent FNF outsourced its data security to LoanCare, FNF made the decision to outsource that duty.

63. Defendants further knew or should have known that if hackers breached their data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, Defendants knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of Defendants' unsecured, unreasonable data security measures.

64. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Defendants to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Defendants' duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendants failing to use reasonable measures to protect sensitive data. Defendants, therefore, were required and obligated to take reasonable measures to protect data they possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendants' duty to adequately protect sensitive personal information. By failing to implement reasonable data security measures, Defendants acted in violation of § 5 of the FTCA.

65. Also, as alleged in further detail below, the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100, imposes an affirmative duty on

businesses, such as Defendants, which maintain personal information about California residents, to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendants failed to implement such procedures which resulted in the Data Breach impacting Plaintiff's and the Class members' sensitive personal information, including PII.

66. Defendants are obligated to perform their business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Defendants to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

67. Finally, Defendants assumed the duty to protect sensitive data by soliciting, collecting, and storing users' data and, additionally, by representing to consumers that it lawfully complied with data security requirements and had adequate data security measures in place to protect the confidentiality of Plaintiff's and the Class's private and sensitive personal information.

68. Defendants breached their duty to Plaintiff and the Class by implementing inadequate and/or unreasonable data security measures that they knew or should have known could cause a Data Breach. Defendants knew or should have known that hackers might target sensitive data Defendants solicited and collected, which was later collected and stored by Defendants, on customers and, therefore, needed to use reasonable data security measures to protect against a Data Breach. Indeed, Defendants acknowledged they were subject to certain standards to protect data and utilize other industry standard data security measures.

69. Defendants were fully capable of preventing the Data Breach. Defendants knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. Defendants particularly were

on notice of inadequate data security measures as LoanCare had experienced a data breach approximately one year ago, which it announced in or around August 2022. Defendants thus failed to take reasonable measures to secure its system, leaving Plaintiff and the Class members' sensitive personal information and/or PII vulnerable to a breach.

70. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

71. Plaintiff and the Class members have suffered damages as a result of Defendants' negligence, including actual and concrete injuries and will suffer additional injuries in the future, including economic and non-economic damages from invasion of privacy, costs related to mitigating the imminent risks of identity theft, time and effort related to mitigating present and future harms, actual identity theft, the loss of the benefit of bargained-for security practices that were not provided as represented, and the diminution of value in their PII.

COUNT II

Negligence Per Se

72. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

73. Defendants' unreasonable data security measures constitute unfair or deceptive acts or practices in or affecting commerce in violation Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, it requires businesses to institute reasonable data security measures and breach notification procedures, which Defendants failed to do.

74. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendants of failing to use reasonable measures to protect users' sensitive data.

75. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the sensitive nature and amount of data Defendants stored on their users and the foreseeable consequences of a Data Breach should Defendants fail to secure their systems.

76. Defendants' violation of Section 5 of the FTC Act constitutes negligence per se.

77. In addition, the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §§ 1798.100, *et seq*. requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." 1798.81.5(c).

78. Defendants violated the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Defendants failed to implement reasonable security procedures and practices to prevent an attack on its servers or systems by hackers and to prevent unauthorized access and exfiltration of Plaintiff's and Class members' PII as a result of the Data Breach.

79. Plaintiff and the Class are within the class of persons Section 5 of the FTC Act, the CCPA, and other similar state statutes, was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act. The CCPA, and other similar state statutes, was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

80. As a direct and proximate result of Defendants' negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT III

Breach of Contract

81. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

82. Plaintiff and Class members entered into a valid and enforceable contract through which they were required to turn over their sensitive personal information to Defendants in exchange for services.

83. That contract included promises by Defendants to secure, safeguard, and not disclose Plaintiff's and Class members' sensitive personal information to any third parties without their consent.

84. Defendants' Privacy Notice published on FNF's website[18] memorialized the rights and obligations of Defendants and its customers. This document was provided to Plaintiff and Class members in a manner in which it became part of the agreement for services with Defendants.

85. Aside from state and federal laws, regulations, and industry standards, through the Privacy Notice, Defendants committed to protecting the privacy and security of the sensitive personal information and promised to never share Plaintiff's and Class members' PII except under certain limited circumstances.

86. Plaintiff and Class members fully performed their obligations under their contracts with Defendants. However, Defendants failed to secure, safeguard, and/or keep private Plaintiff's and Class members' PII, and therefore Defendants breached their contracts with Plaintiff and Class members.

87. Despite Defendants' knowledge of LoanCare's inadequate data security measures that resulted in at least one previously known data breach announced to

[18] https://fnf.com/privacy-notice

customers in August 2022, Defendants continued to store and maintain possession and control of Plaintiff's and Class members' PII, which predictably led to criminal third parties accessing, copying, and or exfiltrating Plaintiff's and Class members' PII without permission through Defendants' failure to reasonably safeguard such data and/or FNF's failure to sufficiently supervise its subsidiary, LoanCare, in doing the same in order to prevent the Data Breach. Therefore, Defendants breached their contracts with Plaintiff and Class members.

88. Defendants' failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTC Act, resulted in Defendants providing services to Plaintiff and Class members that were of a diminished value and in breach of its contractual obligations to Plaintiff and Class members.

89. As a result, Plaintiff and Class members have been harmed, damaged, and/or injured as described herein, including by Defendants' failure to fully perform its part of the agreement with Plaintiff and Class members.

90. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members suffered and will continue to suffer damages in an amount to be proven at trial.

91. In addition to monetary relief, Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security monitoring and supervision procedures, conduct periodic audits of those procedures, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT IV

Breach of Implied Contract

92. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

93. Defendants provide mortgage services to Plaintiff and Class members. Plaintiff and Class members formed an implied contract with Defendants regarding

the provision of those services through its collective conduct, including by Plaintiff and Class members providing their PII to Defendants in exchange for the services offered.

94. Through Defendants' offering of these services, it knew or should have known that it needed to protect Plaintiff's and Class members' confidential PII in accordance with their own policies, practices, and applicable state and federal law.

95. As consideration, Plaintiff and Class members turned over valuable PII relying on Defendants to securely maintain and store their PII in return and in connection with their services.

96. Defendants accepted possession of Plaintiff's and Class members' PII for the purpose of providing services, including data security, to Plaintiff and Class members.

97. In delivering their PII to Defendants in exchange for their services, Plaintiff and Class members intended and understood that Defendants would adequately safeguard their PII as part of those services.

98. Defendants' implied promises to Plaintiff and Class members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to PII, including its business associates, vendors, and/or suppliers, also protect the confidentiality of that data; (2) taking steps to ensure that the PII that is placed in the control of its business associates, vendors, and/or suppliers is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees, business associates, vendors, and/or suppliers; (4) designing and implementing appropriate retention policies to protect the PII against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

99. Plaintiff and Class members would not have entrusted their PII to Defendants in the absence of such an implied contract.

100. Had Defendants disclosed to Plaintiff and the Class that they did not have adequate data security and data supervisory practices to ensure the security of their sensitive data, including but not limited to Defendants' decision to continue to collect, store, and maintain Plaintiff's and Class members' PII despite LoanCare's previous data breach, Plaintiff and Class members would not have agreed to provide their PII to Defendants.

101. As providers of lending and mortgage servicing operations, Defendants recognized (or should have recognized) that Plaintiff's and Class member's PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and the Class.

102. Defendants violated these implied contracts by failing to employ reasonable and adequate security measures and supervision of its vendors, business associates, and/or suppliers to secure Plaintiff's and Class members' PII.

103. A meeting of the minds occurred, as Plaintiff and Class members agreed, *inter alia*, to provide their accurate and complete sensitive personal information to Defendants in exchange for Defendants agreement to, *inter alia*, protect their PII.

104. Plaintiff and Class members have been damaged by Defendants' conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT VI

Breach of Fiduciary Duty

105. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

106. A relationship existed between Plaintiff and Class members and Defendants in which Plaintiff and Class members put their trust in Defendants to protect the PII of Plaintiff and Class members and Defendants accepted that trust.

107. Defendants breached the fiduciary duties that they owed to Plaintiff and Class members by failing to act with the utmost good faith, fairness, and honesty,

failing to act with the highest and finest loyalty, and failing to protect the PII of Plaintiff and Class members.

108. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiff and Class members.

109. But for Defendants' breach of fiduciary duty, the damage to Plaintiff and Class members would not have occurred.

110. Defendants' breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class members.

111. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiff are entitled to and demand actual, consequential, and nominal damages, and injunctive relief.

COUNT VII

Unjust Enrichment

112. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

113. Plaintiff and Class members conferred a benefit on Defendants. Specifically, they provided Defendants with their PII, which PII has inherent value. In exchange, Plaintiff and Class members should have been entitled to Defendants' adequate protection and supervision of their PII, especially in light of their special relationship.

114. Defendants knew that Plaintiff and Class members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the PII entrusted to them. Defendants profited from Plaintiff's retained data and used Plaintiff's and Class members' PII for business purposes.

115. Defendants failed to secure Plaintiff's and Class members' PII and, therefore, did not fully compensate Plaintiff or Class members for the value that their PII provided.

116. Defendants acquired the PII through false promises of data security

and/or inequitable record retention as it failed to disclose the inadequate data security practices, procedures, and protocols previously alleged.

117. If Plaintiff and Class members had known that Defendants would not use adequate data security practices, procedures, and protocols to secure their PII, they would have endeavored to make alternative mortgage servicing choices that excluded Defendants.

118. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class members conferred upon them.

119. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have suffered and/or will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

120. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful

conduct alleged herein. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

121. Plaintiff and Class members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VIII

Declaratory and Injunctive Relief

122. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

123. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

124. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendants' common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Defendants' actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

125. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed, and continue to owe a legal duty to secure the sensitive personal information with which they are entrusted, specifically including information obtained from its customers, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. Defendants breached, and continue to breach, their legal duty by failing to employ reasonable measures to secure their customers' personal information; and,

c. Defendants' breach of their legal duty continues to cause harm to Plaintiff and the Class.

126. The Court should also issue corresponding injunctive relief requiring Defendants to employ adequate security protocols consistent with industry standards to protect its users' data.

127. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendants' data systems. If another breach of Defendants' data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

128. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued.

129. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

///

///

///

///

PRAYER FOR RELIEF

130. Wherefore, Plaintiff, on behalf of themself individually and the Class, requests that this Court award relief as follows:

a. An order certifying the Class and designating Plaintiff as the Class Representative and their counsel as Class Counsel;

b. An award to Plaintiff and the proposed Class members of damages and equitable relief with pre-judgment and post-judgment interest;

c. A declaratory judgment in favor of Plaintiff and the Class;

d. Injunctive relief to Plaintiff and the Class;

e. An award of attorneys' fees and costs as allowed by law; and

f. Any other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

Plaintiff hereby demand a jury trial for all claims and issues so triable.

Dated: December 12, 2023

Respectfully submitted,

By: __/s/ Abbas Kazerounian_____

Abbas Kazerounian
Mona Amini
KAZEROUNI LAW GROUP, APC
245 Fischer Avenue, Suite D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
Email: ak@kazlg.com
Email: mona@kazlg.com

BLOOD HURST & O'REARDON, LLP
Timothy G. Blood
Jennifer L. MacPherson
501 West Broadway, Suite 1490
San Diego, California 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101
tblood@bholaw.com
jmacpherson@bholaw.com

Attorneys for Plaintiff